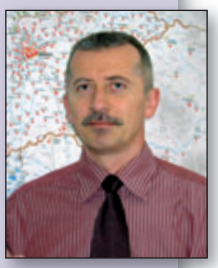

A BIZTONSÁG ELMÉLETE ÉS GYAKORLATA – ZÓLYOMI ZSOLT BIZTONSÁGI VEZETŐT KÉRDEZZÜK

– Információbiztonság, na és a hackerek? – Mit kell védeni és hogyan? – Adatosztályozás, védhető e-mail?

Várjuk Olvasóink aktuális, érdekes, fogós kérdéseit!

■ ***Folytatván beszélgetésünket, rögtön javasolnék is egy témakört, amelyet eddig csak érintettünk, és még nem tudtunk behatóbban foglalkozni vele, ez lenne az információbiztonság.***

– Részemről, semmi akadálya, sőt, kifejezetten szükséges a biztonság egyik meghatározó eleméről beszélnünk, hiszen ma már nem lehet biztonságról értekezni az információbiztonság mellőzésével. Emlékszünk még azokra az időkre, amikor még csak a papír alapú dokumentumok, stencilezett példányok, illetve az indigók védelmével, azok megsemmisítésével foglalkozott a TÜK, vagyis a Titkos Ügyirat Kezelés. Mostanában, bár még mindig fellelhetőek TÜK szabályok szerint tevékenykedő szervezetek, főleg az állami szférában, az információbiztonság ennél már jóval többet jelent. A másik véglet az úgynevezett „paperless" azaz papírmentes folyamatok, ahol már egyáltalán nem keletkezik papír alapú dokumentum, már minden számítógépeken, a virtuális térben történik. Ezek valóban a végletek, a legtöbb szervezetnél, vállalatnál mind a papír alapú, mind a digitális információ megtalálható, és ezek védelméről gondoskodni kell!

■ ***Ha javasolhatnám, akkor nézzük is a témával kapcsolatos első kérdést, amelyben meglehetősen szkeptikus vélemény tükröződik, úgy szól: „Van-e értelme egyáltalán az információk védelmének, hiszen minden rendszert feltörnek a hackerek, ezáltal minden információhoz hozzáférhetnek mások is, nem szélmalomharc a védekezés?!"***

– Valóban sok tehetséges hacker, vagy hacker szervezet létezik, de ők sem mindentudóak. A hackertevékenység általában a nem megfelelően védett rendszerek ellen irányul, ahol nincs minden teljesen lefedve. A rendszerben található hibákat, lyukakat támadják, és azokon keresztül szerezhetnek meg jogosulatlanul információkat, adatokat. A tapasztalatom azt mutatja, hogy egy gondosan megtervezett, megvalósított és üzemeltetett rendszerbe nem tudnak bejutni jogosulatlanul. Természetesen ehhez hozzátartozik, hogy az üzemeltetésnek ki kell terjedni a folyamatos felülvizsgálatokra, fejlesztésekre is, és szakadatlanul figyelni kell a rendszert, itt főleg nem emberi tevékenységre gondolok, hanem speciális IT rendszerekre, amelyek minden a hálózatba érkezett kérést rögzítenek (logolnak), és elemeznek, ha valamit gyanúsnak tartanak, akkor automatikusan, késedelem nélkül riasztanak, igényelve az emberi beavatkozást.

■ ***Hogyan foglalná össze a legfontosabb feladatokat az információbiztonsági rendszer kialakításánál?***

– Mi is az, amit védeni kell? Biztosítani kell az adatok bizalmasságát, az információ csak azok számára legyen elérhető, akik erre jogosultak, biztosítani kell az információk integritását, az információk sértetlenségét, valamint az információk folyamatos rendelkezésre állását, hogy mindig elérhetőek legyenek. Kezdeném a fizikai biztonsági követelmények kialakításával. Legyen szabályozva, hogy kik hova léphetnek be, vagyis legyen egy jól működő beléptetőrendszer, biztonságtechnikai háttér, illetve biztonsági személyzet, őrség, amelyek ezt biztosítani tudják. Szabályozni szükséges a kulcsrendszert, szintén a ki hova tud bejutni szabályozáshoz térnék vissza. Ehhez javasolnék egy szigorúan szabályozott mesterkulcsrendszert. Ezután lehet komolyabban foglalkozni az információbiztonsággal. Alapkövetelmény a szükséges tűzfalak és vírusvédő alkalmazások beüzemelése, ezek hiányában minden támadás akadálytalanul érheti el a rendszereket, aminek a következménye a rendkívül rövid idő alatt bekövetkező teljes rendszerösszeomlás. Következő lépés az adatok felmérése, azaz milyen adatokról, ezek mennyire nyíltak, vagy bizalmasak, és mekkora adatmennyiségről van szó, majd ez alapján meg lehet tervezni az adatosztályozási rendszert. Az adatosztályozás fontosságára kiemelten felhívnám a figyelmet, mert ez a rendszer, majd szabályzat fogja meghatározni, hogy milyen dokumentumokat, hogyan szükséges védeni. A vállalkozás tevékenységétől nagymértékben függ, hogy milyen rendszer számára az ideális. A legegyszerűbb a kétszintű adatosztályozás, amely a nyílt és a bizalmas adatok kezelésének szabályait írja elő, de ismertek ennél sokkal bonyolultabb több szintű adatosztályozások is, például egy ötszintű osztályozás, ami állhat szigorúan titkos, titkos, bizalmas, belsőhasználatú, illetve nyílt adatokból. Véleményem szerint mindig a legegyszerűbb rendszerek a legműködőképesebbek, de elképzelhető, hogy a cég tevékenysége megkívánja a többszintű rendszer működtetését.

■ ***Megvizsgálhatnánk egy közepes szintű adatosztályozási rendszert egy kicsit részletesebben?***

– Épp javasolni szerettem volna, tehát nézzünk egy háromszintű rendszert! A három szint legyen alulról kezdve a következő: első szint a nyílt, azaz publikus információkat tartalmazó szint lenne, a másodikat nevezzük belső használatú dokumentumoknak, és a harmadik, a legszigorúbb szint legyen a bizalmas minősítésű adatok köre. Ezennel beazonosítottuk, vagyis felmértük az adataink körét, most ezekhez szükséges kialakítani a védelmi szintet. Elő kell írnunk, hogy mi a teendő ilyen dokumentumok védelmével kapcsolatban. Értelemszerűen a nyílt, publikus adatok számára nem írunk elő semmilyen védelmet, hiszen, ezeket az információkat minden korlátozás nélkül meg lehet osztani külsősökkel, harmadik féllel, stb. A második szintű dokumentumok esetében már elő kell írnunk, hogy ezekhez a dokumentumokhoz csak cégünk dolgozói férhetnek hozzá. Ezeket külső személyek részére átadni, kiküldeni, stb. nem lehet. Ezeket a dokumentumokat kizárólag a cég szerverein, számítógépein lehet tárolni, kinyomtatott példányait nem lehet a cég területéről kivinni. A harmadik, a bizalmas dokumentumok szintje, vagyis ezek a dokumentumok a cégen belül sem elérhetőek mindenki számára, csak egy meghatározott, bizalmas körnek, akiknek az információ szól. Értelemszerűen ez a kör mindig más, attól függően, hogy kihez szól, illetve kire tartozik az a bizalmas adat, vagy információ. Ebben a példában említett esetben ezekhez a harmadik szintű dokumentumokhoz kell létrehozni a legmagasabb szintű védelmi rendszert, amely garantálja, hogy csak az arra jogosultak férhetnek hozzá az adatokhoz. Előírhatjuk, hogy ezen dokumentumok csak egy addicionális védelemmel ellátott szerveren tárolhatóak (erre többféle technikai megoldás is elérhető), kinyomtatott példányaikat csak mások által hozzá nem férhető helyen, elzárva kell tartani.

■ ***Igen, de mi történik abban az esetben, ha e-mailben szükséges olyan adatokat továbbküldenünk, amelyeket nem szeretnénk másokkal megosztani, hogyan ítéli meg az e-mailek biztonságát?***

– Kérdésével már rá is tértünk egy másik fontos területre, az e-mailek biztonságára. Én

nem küldenék sima e-mailben bizalmas adatokat, mert ezzel igen nagy rizikót vállalnék. Szerencsére már elérhetőek olyan rendszerek, amelyek az elektronikus levelezés biztonságát tudják szavatolni, mint például a PKI (Public Key Infrastructure, Publikus Kulcsú Technológia). Ez már olyan titkosítási algoritmusokat tartalmazó azonosítási eljárás, ami a mai eszközökkel nem törhető fel. A rendszer által biztosított, hogy csak a címzett tudja elolvasni a levelet, mások számára hozzáférhetetlen marad az információ.

■ ***A technikai megoldások mellett milyen egyéb eljárásokat javasol, amelyek segíthetik a bizalmas információk megőrzését?***

– A „Clean Desk Policy"-t, a Tiszta Asztal Folyamatot nem győzöm eléggé hangsúlyozni, hogy mennyire fontos a betartása, illetve a betartatása. Lényege, hogy mindenkinek gondoskodni kell arról, hogy amikor elhagyja a munkahelyét, akár csak egy percre is, akkor is, és mindenkor zárja le a számítógépét, a jelszó ismeretének hiánya miatt más ne tudjon hozzáférni a gépén tárolt adatokhoz, illetve mások által hozzá nem férhető helyre zárja el a bizalmas dokumentumait. Ezeket minden esetben meg kell tennie minden dolgozónak. A folyamat betartását a biztonsági szervezetnek ellenőrizni kell munkaidő után és az ellenőrzés tapasztalataira értesíteni kell a munkahelyi vezetőt, illetve a vezetőséget, akiknek el kell járni a vétkesekkel szemben a vállalati bizalmas információk védelmében. Említettem már a fizikai biztonsági folyamatokat, de szeretném felhívni a figyelmet arra, hogy elengedhetetlenül fontos a takarítás, a karbantartás, illetve hasonló folyamatok biztonsági szabályzása, mert felügyelet nélkül elég sok minden megtörténhet. Végezetül ne feledkezzünk meg a humánbiztonság jelentőségéről sem, mert el kell tudnunk hárítani, hogy a rendszerben a leggyengébb láncszem az ember legyen, de ez már egy másik feladatkör.

■ ***Mindig eltűnődöm azon, hogy mennyi mindent kell számításba venni, amikor egy kérdést szeretnénk teljesen megoldani, leszabályozni, köszönöm a mai beszélgetést!***

K. M.